Release A CDR RID Report

Date Last Modified 12/12/95
Originator Belton, Muata
Organization CSC
E Mail Address mblelton@ulabsgi.gsfc.nasa.gov
Document DDDR

Phone No (301)794-1698

RID ID **CDR** 100
Review DDDR
Originator Ref NA
Priority 2

Section PLANG Components **Page** KL-19 **Figure Table** NA

Category Name Planning (PLS) Design **Actionee** ECS

Sub Category

Subject Planning Workbench Security

Description of Problem or Suggestion:

A security conceptual design and its related security services were not presented for the Planning Workbench at the DDDR. This problems is consistence with CDR RID #53, whereas security vulnerabilities exist in the use of UNIX-X-Windows displays in a multi-user system environment. The 'xhost' command in UNIX allows anyone who can log into (or break into) your system to run programs on your display has the capability to perform the following attacks and most of these can be done with no warning and leaving no trace:
1. Destroying any (or all) of your windows:
2. Opening new windows on your screen:
3. Viewing the contents of your screen remotely;
4. Logging keystrokes (including passwords); and
5. Generating spurious X events remotely.

Originator's Recommendation

A security conceptual design is required forthe Planning Workbench CI and a textual description of the security services used in the Workbench GUIs which will employ X-Window security safeguards.

GSFC Response by: **GSFC Response Date**

HAIS Response by: Richard Meyer **HAIS Schedule** 10/25/95

HAIS R. E. Richard Meyer **HAIS Response Date** 11/28/95

The Client subsystem will be deployed in two major configuration variants.

ï The first is the ECS DAAC configuration. It will be used to support operations personnel.

ï The second is the SCF configuration, which is available to support general users outside of the ECS perimeter.

To protect the X environment in the first configuration against intrusions such as those described in the RID, address filtering will be used to disallow any X traffic from sources outside the ECS DAACs. The network topology and network security is described in Section 5.5 of 305-CD-004-001 (see, for example, Figure 5.5-3). In addition, ECS has special arrangements with the instrument teams to permit direct X access from their locations to the Planning Subsystem application. This access will be protected against intrusion by using either private or switched dial in circuits, or special routers at the respective SCFs to isolate the workstations authorised for such access. None of the other Client configurations deployed at SCFs or other users will have such direct X access capability.

ECS has no authority or responsiblity for the security policy and measures at the installations which will use the SCF Client configurations (other than as indicated above). These installations are outside the scope of ECS Security.

Status **Closed** **Date Closed** **12/12/95** **Sponsor** **Kempler**

****** **Attachment if any** ******